UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
SEATTLE DIVISION

MARIANNA POWERS, on behalf of herself and all others similarly situated, Plaintiff, vs. PREMERA BLUE CROSS, a Washington corporation, Defendant.	Case No. CLASS ACTION **COMPLAINT—CLASS ACTION** DEMAND FOR JURY TRIAL

PHILLIPS LAW FIRM PLLC
17410 133rd Ave NE, Suite 301, Woodinville WA 98072
Tel: (425) 482-1111 Fax: (425) 482-6653

SUMMARY OF THE CASE

1. On March 17, 2015, Premera Blue Cross announced that hackers had breached the company's systems and obtained the personal and medical information of approximately 11 million current and former Premera health insurance plan members, employees, and members of other Blue Cross Blue Shield plans who sought treatment in Washington or Alaska. The personal information compromised in the breach includes names, birthdates, Social Security numbers, member identification numbers, addresses, email addresses, bank account information, and medical claims information, including clinical information.

2. Plan members' and employees' personal and medical information has been exposed – and their identities put at risk – because Premera failed to maintain reasonable and adequate security measures. Although Premera has statutory obligations to protect the sensitive personal information it maintains, it failed at numerous opportunities to prevent, detect, or limit the scope the breach. Among other things, Premera (1) failed to implement preventative security measures even though the healthcare industry has been repeatedly warned about the risk of cyber-attacks, and (2) failed to employ security protocols to detect the unauthorized network activity. Moreover, after discovering the data breach, Premera waited over six weeks to begin notifying members and employees whose personal information was affected.

3. Plaintiff Marianna Powers is a current Premera plan member who brings this proposed class action lawsuit on behalf of former and current members of a Premera health insurance plan, and employees whose personal and medical information has been compromised as a result of the data breach. She seeks injunctive relief requiring Premera to implement and maintain security practices to comply with regulations designed to prevent and remedy these types of breaches, as well as damages, and other relief.

PARTIES

4. Plaintiff Marianna Powers is a citizen and resident of Yakima County, Washington.

5. Defendant Premera Blue Cross ("Premera") is a Washington corporation with its principal place of business in Snohomish County, Washington.

PHILLIPS LAW FIRM PLLC
17410 133rd Ave NE, Suite 301, Woodinville WA 98072
Tel: (425) 482-1111 Fax: (425) 482-6653

JURISDICTION AND VENUE

6. This Court has original jurisdiction pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d), because (a) at least one member of the proposed class is a citizen of a state different from Premera, (b) the amount in controversy exceeds $5,000,000, exclusive of interest and costs, (c) the proposed class consists of more than 100 class members, and (d) none of the exceptions under the subsection apply to this action.

7. This Court has jurisdiction over Premera because it is registered to conduct business in Washington, has sufficient minimum contacts in Washington, or otherwise intentionally avails itself of the markets within Washington, through the promotion, sale, marketing and distribution of its products in Washington, such that the exercise of jurisdiction by this Court is proper and necessary.

8. Venue is proper in this District under 28 U.S.C. § 1391 because Premera resides in this district, conducts substantial business in this District, and a substantial part of the events giving rise to Plaintiff's claims occurred in this District.

INTRADISTRICT ASSIGNMENT

9. Assignment is proper to the Seattle division of this District under Local Rule 3(d)(1) as a substantial part of the events and omissions giving rise to Plaintiff's claims occurred in Snohomish County.

FACTUAL ALLEGATIONS

The Data Breach

10. Premera is a major provider of healthcare services. Premera collects and stores its members' and employees' personal and medical information on its computer servers. Premera maintains a Notice of Privacy Practices that promises the company "is committed to maintaining the confidentiality of [its members'] medical and financial information."[1] This policy also claims that Premera would protect members' personal information in a variety of ways:

[1] Premera Notice of Privacy Practices, https://www.premera.com/wa/visitor/privacy-policy/ (last visited Apr. 1, 2015).

PHILLIPS LAW FIRM PLLC
17410 133rd Ave NE, Suite 301, Woodinville WA 98072
Tel: (425) 482-1111 Fax: (425) 482-6653

> For example, we authorize access to your personal information by our employees and business associates only to the extent necessary to conduct our business of serving you, such as paying your claims. We take steps to secure our buildings and electronic systems from unauthorized access. We train our employees on our written confidentiality policy and procedures and employees are subject to discipline if they violate them. Our privacy policy and practices apply equally to personal information about current and former members; we will protect the privacy of your information even if you no longer maintain coverage through us.[2]

11. On March 17, 2015, the company announced that hackers had breached its network, compromising the personal information of approximately 11 million Premera health insurance plan members, employees, and those with whom Premera does business. Approximately 6 million of those affected are Washington residents with the remainder residing in various states across the country.[3] The incident affected Premera Blue Cross, Premera Blue Cross Blue Shield of Alaska, its affiliate brands Vivacity and Connexion Insurance Solutions, Inc., and members of other Blue Cross Blue Shield plans who sought treatment in Washington or Alaska.[4] The compromised information goes as far back as 2002 and includes names, birthdates, Social Security numbers, member identification numbers, addresses, email addresses, bank account information, and medical claims information, including clinical information.[5]

12. According to Premera, the initial cyber-attack occurred on May 5, 2014.[6] However, Premera did not discover the attack until January 29, 2015[7] and did not begin notifying

---

[2] *Id.*

[3] Jim Finkle, *Premera Blue Cross breached, medical information exposed*, REUTERS (Mar. 17, 2015, 5:04 PM) http://www.reuters.com/article/2015/03/17/us-cyberattack-premera-idUSKBN0MD2FF20150317.

[4] *Premera has been the target of a sophisticated cyberattack*, Premera, http://www.premeraupdate.com (last visited Apr. 2, 2015).

[5] Elise Viebeck, *Federal workers might be victims of Premera data breach*, THE HILL (Mar. 19, 2015, 11:27 AM) http://thehill.com/policy/cybersecurity/236266-federal-workers-might-be-victims-of-premera-breach.

[6] Mike Baker, *Feds warned Premera about security flaws before breach*, THE SEATTLE TIMES (Mar. 18, 2015, 11:04 AM) http://www.seattletimes.com/business/local-business/feds-warned-premera-about-security-flaws-before-breach/.

[7] Anna Wilde Mathews & Danny Yadron, *Premera Blue Cross Says Cyberattack Could Affect 11 Million Members*, THE WALL STREET JOURNAL (Mar. 17, 2015, 10:28 PM) http://www.wsj.com/articles/premera-blue-cross-says-cyberattack-could-affect-11-million-members-1426627752.

PHILLIPS LAW FIRM PLLC
17410 133rd Ave NE, Suite 301, Woodinville WA 98072
Tel: (425) 482-1111 Fax: (425) 482-6653

affected members until March 17, 2015. As a result of the six-week delay in providing proper notice regarding the data breach, many class members have been unaware that their personal information has been compromised and therefore have not timely taken the steps necessary to safeguard themselves from the improper use of that information.

Premera's Security Practices are Inadequate

13. In January and February 2014, the United States Office of Personnel Management ("OPM") conducted an on-site audit of Premera's systems and security controls.[8] In April 2014, OPM informed Premera of several concerns in connection to the company's network security controls, including "that patches [we]re not being implemented in a timely manner," that "[a] methodology [wa]s not in place to ensure that unsupported or out-of-date software [wa]s not utilized," and that "[i]nsecure server configurations were identified in a vulnerability scan" which could give hackers access to sensitive information.[9] Moreover, the report indicated that "Premera's data center did not contain controls [] typically observe[d] at similar facilities, such as multi-factor authentication and piggybacking prevention" to prevent unauthorized persons to gain entry into its systems.[10]

14. On June 30, 2014, Premera responded to the audit, stating that it had made some changes and planned to implement further changes by December 31, 2014. However, the breach had already begun on May 5th.

15. Healthcare providers are frequently the targets of cyber-attacks because their networks store large amounts of sensitive personal information. Unlike credit card and bank account numbers, information maintained by healthcare companies – such as birthdates and Social Security numbers – is not easily destroyed and can be used to perpetrate identify theft and other types of frauds. Medical information is also far more valuable on the black market than credit card or other personal information, and businesses that store such information are therefore

[8] *Final Audit Report – Audit of Information Systems Genera and Application Controls at Premera Blue Cross*, U.S. OFFICE OF PERSONNEL MANAGEMENT, 2 (Nov. 28, 2014), *available at* http://www.opm.gov/our-inspector-general/reports/2014/audit-of-inoformation-systems-general-and-application-controls-at-premera-blue-cross.pdf.
[9] *Id.* at ii.
[10] *Id.* at 4-5.

PHILLIPS LAW FIRM PLLC
17410 133rd Ave NE, Suite 301, Woodinville WA 98072
Tel: (425) 482-1111 Fax: (425) 482-6653

likely to be targeted by cybercriminals. According to Dave Kennedy, a healthcare security expert, "Medical records paint a really personal picture of somebody's life and medical procedures . . . [and] allow [a criminal] to perpetrate really in-depth medical fraud."[11] Medical information is highly valuable and is reportedly "worth 10 times more than [a person's] credit card number on the black market."[12] A report prepared by the Ponemon Institute estimated that 90% of healthcare organizations have incurred at least one data breach over the last two years.[13]

16. On April 8, 2014, the Federal Bureau of Investigation issued a Private Industry Notification to healthcare providers, warning them that their cybersecurity systems are inadequate.[14] According to the notification, "[t]he healthcare industry is not as resilient to cyber intrusions compared to the financial and retail sectors, therefore the possibility of increased cyber intrusions is likely." Particularly in light of recent data breaches at numerous large retailers and healthcare providers – including Target, Home Depot, Anthem, and Community Health Systems – Premera knew or should have known that its computers systems were vulnerable and should have been more vigilant than ever of the need to adopt, implement, and maintain security measures to protect its members' and employees' personal information.

17. The FBI notification also cites a report prepared by the SANS Institute that warned that the healthcare industry was not sufficiently prepared to combat cyber-attacks. The SANS Health Care Cyber Threat Report analyzed data collected between September 2012 and 2013 and found the results to be "alarming."[15] The report explained that "[t]he data not only

---

[11] Finkle, *supra* note 3.

[12] Caroline Humer & Jim Finkle, *Your medical record is worth more to hackers than your credit card*, REUTERS (Sept. 24, 2014, 2:24 PM), http://www.reuters.com/article/2014/09/24/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924.

[13] *Fourth Annual Benchmark Study on Patient Privacy & Data Security*, PONEMON INSTITUTE, 2 (Mar. 2014), *available at* https://www.privacyrights.org/sites/privacyrights.org/files/ID%20Experts%204th%20Annual%20Patient%20Privacy%20&%20Data%20Security%20Report%20FINAL.pdf.

[14] Jim Finkle, *Exclusive: FBI warns healthcare sector vulnerable to cyberattacks*, REUTERS (Apr. 23, 2014, 3:15 PM), http://www.reuters.com/article/2014/04/23/us-cybersecurity-healthcare-fbi-exclusiv-idUSBREA3M1Q920140423.

[15] SANS INSTITUTE, HEALTH CARE CYBERTHREAT REPORT: WIDESPREAD COMPROMISES DETECTED, COMPLIANCE NIGHTMARE ON HORIZON, 2 (Feb. 2014), *available at* http://pages.norse-corp.com/rs/norse/images/Norse-SANS-Healthcare-Cyberthreat-Report2014.pdf.

PHILLIPS LAW FIRM PLLC
17410 133rd Ave NE, Suite 301, Woodinville WA 98072
Tel: (425) 482-1111 Fax: (425) 482-6653

confirmed how vulnerable the industry had become, it also revealed how far behind industry-related cybersecurity strategies and controls have fallen."

18. In August 2014 – after a cyber-attack on Community Health Systems, Inc. – the FBI warned companies within the healthcare industry that hackers were targeting them.[16] The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."

19. Despite receiving notice that its systems were inadequate to protect sensitive information, that hackers were increasing their efforts to access personal information maintained by healthcare companies, and that the healthcare industry should therefore emphasize data security, Premera (1) failed to implement preventative security measures despite repeated warnings about the risk of cyber-attacks, and (2) failed to employ security protocols to detect unauthorized network activity. Moreover, after discovering the data breach, Premera waited over six weeks to begin notifying members and employees whose personal information was compromised.

Current and Former Premera Health Plan Members and Premera Employees Are Victims of the Breach

20. As a result of Premera's negligent security practices and the delay in notifying affected customers, former and current Premera health plan members and employees are subject to an increased and concrete risk of identity theft based on the Premera's exposure of their personal information.

21. Former and current Premera plan members and employees will have to spend time and money securing their personal information and protecting their identities. They will need to monitor their accounts and credit, and will also have to pay for credit monitoring or credit reports in the wake of the data breach to make sure that their credit and identity is not harmed by anyone who may have stolen their information. Individuals whose bank accounts are compromised may

[16] Jim Finkle, *FBI warns healthcare firms they are targeted by hackers*, REUTERS (Aug. 20, 2014, 4:32 PM), http://www.reuters.com/article/2014/08/20/us-cybersecurity-healthcare-fbi-idUSKBN0GK24U20140820.

PHILLIPS LAW FIRM PLLC
17410 133rd Ave NE, Suite 301, Woodinville WA 98072
Tel: (425) 482-1111 Fax: (425) 482-6653

have to pay fees to their banks for new debit cards, or have to pay fees to have the cards shipped faster so that they do not have to wait weeks to make purchases on their accounts.

22. The disclosure of Social Security numbers in particular poses significant risks. Criminals can, for example, use Social Security numbers to create false bank accounts or file fraudulent tax returns. Former and current Premera plan members and employees whose Social Security numbers have been compromised have spent time contacting various agencies, such as the Internal Revenue Service, the Social Security Administration, and their local state tax boards. They also now face a real and immediate risk of identity theft and other problems associated with the disclosure of their Social Security number, and will need to monitor their credit and tax filings for an indefinite duration. Individuals cannot even obtain a new Social Security number *until* there is evidence of ongoing problems due to misuse of the Social Security number. Even then, the Social Security Administration warns "that a new number probably will not solve all [] problems . . . and will not guarantee [] a fresh start." "For some victims of identity theft, a new number actually creates new problems."[17]

23. Although Premera has offered two years of free credit monitoring and identity theft protection services to its members and customers, according to cyber-security expert Brian Seely, "it's likely not long enough" since birth dates and Social Security numbers were stolen.[18] The information exposed in the Premera data breach is sufficient for criminals to "get loans, commit tax fraud, medical identity theft, child identity theft . . ., synthetic identity theft and criminal identity theft," stated Adam Levin, who is the chairman and co-founder of Credit.com and former director of the New Jersey Division of Consumer Affairs.[19] According to Mr. Levin, "Premera customers will be forced to look over their shoulders for the rest of their lives."

[17] *Identity Theft And Your Social Security Number*, Social Security Administration (Dec. 2013), *available at* http://www.ssa.gov/pubs/EN-05-10064.pdf.

[18] Elisa Hahn, *More people join class action lawsuits against Premera*, KING 5 NEWS (Mar. 31, 2015), http://www.king5.com/story/news/local/2015/03/31/premera-cyber-security-data-breach-class-action-lawsuit/70748850.

[19] *Health insurer Premera hit by "sophisticated cyberattack,"* MONEYWATCH, CBS NEWS (last updated Mar. 17, 2015, 6:45 PM), http://www.cbsnews.com/news/health-insurer-premera-hit-by-sophisticated-cyberattack/.

PHILLIPS LAW FIRM PLLC
17410 133rd Ave NE, Suite 301, Woodinville WA 98072
Tel: (425) 482-1111 Fax: (425) 482-6653

24. Third party criminals have already taken advantage of the Premera data breach in an attempt to obtain class members' personal information. Some class members have already received notices that fraudulent tax returns were filed in their names.[20]

25. Premera has provided little information about how affected customers can protect themselves. Other than advising its members to sign up for Premera's free credit monitoring and identity protection services, its website provides no other information or guidance about what steps class members can take to protect their identities and minimize the damage arising from the data breach.[21]

PLAINTIFF POWERS'S EXPERIENCE

26. Plaintiff Marianna Powers is a resident of Yakima County, Washington. Ms. Powers works for the United States Postal Service and has health insurance coverage through Premera for herself and her husband. Ms. Powers and her husband became members of a Premera health insurance plan in or around 2013. Premera obtained their sensitive personal information, including their birthdates, Social Security numbers, address, email addresses, and employment information.

27. Plaintiff Powers learned of the Premera data breach from her employer and then from news media. About two to three weeks after news media sources first reported on the data breach, Ms. Powers received a letter from Premera notifying her of the data breach.

28. The Premera data breach has compromised the personal data of Ms. Powers and her husband, including their birthdates, medical IDs, Social Security numbers, address, and email addresses. Due to Premera's conduct, Plaintiff Powers and her husband are now at a heightened risk for future identity theft.

CLASS ACTION ALLEGATIONS

29. Plaintiff brings this action pursuant to Federal Rule of Civil Procedure 23 on behalf of herself and the classes preliminarily defined as:

[20] *See* Hahn, *supra* note 18.
[21] *See* Premera, *supra* note 4.

PHILLIPS LAW FIRM PLLC
17410 133rd Ave NE, Suite 301, Woodinville WA 98072
Tel: (425) 482-1111 Fax: (425) 482-6653

Washington Class

Current and former members of a Premera health insurance plan and Premera employees in Washington whose personal information was compromised as a result of the data breach announced in March 2015.

Nationwide Class

Current and former members of a Premera health insurance plan and Premera employees in the United States whose personal information was compromised as a result of the data breach announced in March 2015.

Excluded from the proposed classes are anyone employed by counsel for Plaintiff in this action and any Judge to whom this case is assigned, as well as his or her staff and immediate family.

30. Plaintiff satisfies the numerosity, commonality, typicality, and adequacy prerequisites for suing as a representative party pursuant to Rule 23.

31. Numerosity. The proposed classes consist of millions of former or current Premera health insurance plan members and employees who had their data stolen in the Premera data breach, making joinder of each individual class member impracticable.

32. Commonality. Common questions of law and fact exist for the proposed classes' claims and predominate over questions affecting only individual class members. Common questions include:

a. Whether Premera violated R.C.W. § 19.255.010 by failing to promptly notify class members that their personal information had been compromised;

b. Whether Premera's failure to adequately protect class members' personal information and promptly notify class members that their personal information had been compromised constitutes as unfair or deceptive practices under the Washington Consumer Protection Act, R.C.W. § 19.86, *et seq.*;

c. Whether Premera acted negligently in failing to maintain adequate security procedures and practices;

d. Whether Premera breached its contractual promises to adequately protect class members' personal information;

PHILLIPS LAW FIRM PLLC
17410 133rd Ave NE, Suite 301, Woodinville WA 98072
Tel: (425) 482-1111 Fax: (425) 482-6653

e. Whether class members may obtain damages, restitution, and injunctive relief against Premera; and

f. What security procedures and data-breach notification procedure Premera should be required to implement as part of any injunctive relief ordered by the Court.

33. Typicality. Plaintiff's claims are typical of the claims of the proposed classes because, among other things, Plaintiff and class members sustained similar injuries as a result of Premera's uniform wrongful conduct and their legal claims all arise from the same core Premera practices.

34. Adequacy. Plaintiff will fairly and adequately protect the interests of the classes. Her interests do not conflict with class members' interests and she has retained counsel experienced in complex class action and data privacy litigation to vigorously prosecute this action on behalf of the classes.

35. In addition to satisfying the prerequisites of Rule 23(a), Plaintiff satisfies the requirements for maintaining a class action under Rule 23(b)(3). Common questions of law and fact predominate over any questions affecting only individual class members and a class action is superior to individual litigation. The amount of damages available to individual plaintiffs is insufficient to make litigation addressing Premera's conduct economically feasible in the absence of the class action procedure. Individualized litigation also presents a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system presented by the legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

36. In addition, class certification is appropriate under Rule 23(b)(1) or (b)(2) because:

a. Prosecution of separate actions by individual members of the proposed classes would create a risk of inconsistent or varying adjudication which would establish incompatible standards of conduct for Premera;

PHILLIPS LAW FIRM PLLC
17410 133rd Ave NE, Suite 301, Woodinville WA 98072
Tel: (425) 482-1111 Fax: (425) 482-6653

b. Prosecution of separate actions by individual members of the proposed classes would create a risk of adjudications which would, as a practical matter, be dispositive of the interests of other class members not parties to the adjudications, or substantially impair or impede their ability to protect their interests; and

c. Premera has acted or refused to act on grounds that apply generally to the proposed classes, thereby making final injunctive relief or declaratory relief described herein appropriate with respect to the proposed classes as a whole.

FIRST CAUSE OF ACTION

For Violation of the R.C.W. § 19.255.010

37. Plaintiff incorporates the above allegations by reference.

38. Plaintiff brings this cause of action on behalf of the Washington Class whose personal information was compromised in the data breach announced in March 2015.

39. This statute requires any business that conducts business in Washington and maintains personal information to disclose "in the most expedient time possible and without unreasonable delay" any security breaches the business discovers. R.C.W. § 19.255.010(1).

40. Pursuant to R.C.W. § 19.255.010(5), "personal information" consists of an individual's first and last name in combination with a Social Security number, driver's license or Washington identification card number, or account or credit card or debit card information.

41. The breach of the personal data of millions of former and current Premera health insurance plan members and employees constitutes a "breach of the security of the system" as defined by R.C.W. § 19.255.010(4).

42. By failing to promptly notify all affected former and current Premera plan members and employees that their personal information had been acquired (or was reasonably believed to have been acquired) by unauthorized persons in the data breach, Premera violated R.C.W. § 19.255.010(1)-(2). Premera's failure to timely notify members and employees of the breach has caused damage to class members who have had to buy identity protection services or take other measures to remediate the breach caused by Premera's negligence.

PHILLIPS LAW FIRM PLLC
17410 133rd Ave NE, Suite 301, Woodinville WA 98072
Tel: (425) 482-1111 Fax: (425) 482-6653

43. By violating R.C.W. § 19.255.010, Premera "may be enjoined" under R.C.W. § 19.255.010(10)(b).

44. Accordingly, Plaintiff requests that the Court enter an injunction requiring Premera to implement and maintain reasonable security procedures to protect members' and employees' data in compliance with the Revised Code of Washington, including, but not limited to: (1) ordering that Premera, consistent with industry standard practices, engage third party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Premera's systems on a periodic basis; (2) ordering that Premera engage third party security auditors and internal personnel, consistent with industry standard practices, to run automated security monitoring; (3) ordering that Premera audit, test, and train its security personnel regarding any new or modified procedures; (4) ordering that Premera, consistent with industry standard practices, conduct regular database scanning and securing checks; (5) ordering that Premera, consistent with industry standard practices, periodically conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and (6) ordering Premera to meaningfully educate its former and current members and employees about the threats they face as a result of the loss of their personal information to third parties, as well as the steps they must take to protect themselves.

45. Plaintiff further requests that the Court require Premera to (1) identify and notify all members of the class who have not yet been informed of the data breach; and (2) notify affected former and current members and employees of any future data breaches by email within 24 hours of Premera's discovery of a breach or possible breach and by mail within 72 hours.

46. As a result of Premera's violation of R.C.W. § 19.255.010, Plaintiff and members of the class have and will incur economic damages relating to time and money spent remedying the breach, including but not limited to, expenses for bank fees associated with the breach, any unauthorized charges made on financial accounts, lack of access to funds while banks issue new cards, tax fraud, as well as the costs of credit monitoring and purchasing credit reports.

PHILLIPS LAW FIRM PLLC
17410 133rd Ave NE, Suite 301, Woodinville WA 98072
Tel: (425) 482-1111 Fax: (425) 482-6653

47. Plaintiff, individually and on behalf of the members of the Washington Class, seeks all remedies available under R.C.W. § 19.255.010, including, but not limited to: (a) damages suffered by members of the class; and (b) equitable relief.

48. Plaintiff, individually and on behalf of the members of the Washington Class, also seek reasonable attorneys' fees and costs under applicable law including Federal Rule of Civil Procedure 23.

SECOND CAUSE OF ACTION

For Unfair Business Practices Under the Washington Consumer Protection Act, R.C.W. § 19.86, *et seq.*

49. Plaintiff incorporates the above allegations by reference.

50. Plaintiff brings this cause of action on behalf the Washington Class whose personal information was compromised as a result of the data breach publicized in March 2015.

51. Premera is a "person" within the meaning of R.C.W. § 19.86.010(1), who conducts "trade" and "commerce" within the meaning of R.C.W.. § 19.86.010(2).

52. Premera's acts and practices, as alleged in this complaint, constitute unfair or deceptive acts or practices, in violation of the R.C.W. § 19.86.020.

53. By failing to safeguard the personal and medical information of Plaintiff and class members, and by failing to promptly notify Plaintiff and class members about the data breach that compromised the personal information of Plaintiff and class members, Premera engaged in unfair acts or practices that offend public policy, as set forth in the Health Insurance Portability and Accountability Act (HIPAA) and other laws, and that are immoral, unethical, oppressive, and/or unscrupulous.

54. "A major goal of the Privacy Rule [under HIPAA] is to assure that individuals' health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and well being."[22] Premera's unfair or deceptive practices violated HIPAA by failing to establish procedures to

[22] OCR Privacy Brief – Summary of the HIPAA Privacy Rule, United States Department of Health and Human Services (last updated May 2003), *available at* http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf.

PHILLIPS LAW FIRM PLLC
17410 133rd Ave NE, Suite 301, Woodinville WA 98072
Tel: (425) 482-1111 Fax: (425) 482-6653

keep members' and employees' medical information confidential and private. Protected health information under HIPAA includes "individually identifiable health information," including name, address, date of birth, and social security number.[23] The Department of Health and Human Services Office of Civil Rights has clarified that "[t]he personally identifiable information health plans maintain on enrollees and members — including names and social security numbers — is protected under HIPAA, even if no specific diagnostic or treatment information is disclosed."[24] 45 C.F.R. § 164.530(c)(1) requires that healthcare providers implement reasonable safeguards for this information, which Premera failed to do. 45 C.F.R. § 164.404 requires that companies provide notice of the breach of unsecured protected health information, which includes protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons. *See* 45 C.F.R. § 164.402. Premera has failed to timely provide such notice.

55. Premera's unfair or deceptive practices have, and are capable of, injuring Plaintiff and class members. As a direct and proximate result of Premera's unfair or deceptive acts or practices as alleged herein, Plaintiff and the class have been injured in that their personal information has been compromised. Plaintiff and class members face an increased risk of identity theft, financial fraud, tax fraud, and medical fraud, based on the theft and disclosure of their personal information. Class members have also lost money and property by purchasing credit monitoring services they would not otherwise had to but for Premera's unfair or deceptive practices.

56. Because of Premera's unfair or deceptive practices, Plaintiff and the class are entitled to relief, including actual damages, treble damages, and a permanent injunction enjoining Premera from its unfair or deceptive practices.

57. The injunctive relief that Plaintiff and members of the class are entitled to includes, but is not limited to: (1) ordering that Premera, consistent with industry standard

[23] *See id.*

[24] Brandon Bailey, Ted Bridis, & Tom Murphy, *Anthem Breach: A Gap in Federal Health Privacy Law?*, N.Y. TIMES (Feb. 6, 2015, 3:36 PM), http://www.nytimes.com/aponline/2015/02/06/us/politics/ap-us-anthem-hack-privacy-law.html?_r=0.

PHILLIPS LAW FIRM PLLC
17410 133rd Ave NE, Suite 301, Woodinville WA 98072
Tel: (425) 482-1111 Fax: (425) 482-6653

practices, engage third party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Premera's systems on a periodic basis; (2) ordering that Premera engage third party security auditors and internal personnel, consistent with industry standard practices, to run automated security monitoring; (3) ordering that Premera audit, test, and train its security personnel regarding any new or modified procedures; (4) ordering that Premera, consistent with industry standard practices, conduct regular database scanning and securing checks; (5) ordering that Premera, consistent with industry standard practices, periodically conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and (6) ordering Premera to meaningfully educate its former and current members and employees about the threats they face as a result of the loss of their personal information to third parties, as well as the steps they must take to protect themselves.

58. Plaintiff, individually and on behalf of the members of the Washington class, also seeks reasonable attorneys' fees and costs under R.C.W. § 19.86.090 and applicable law, including Federal Rule of Civil Procedure 23.

THIRD CAUSE OF ACTION

Breach of Contract

59. Plaintiff incorporates the above allegations by reference.

60. Plaintiff brings this cause of action on behalf of the Nationwide Class whose personal information was compromised as a result of the data breach publicized in March 2015.

61. Premera's Notice of Privacy Practices promises that the company "is committed to maintaining the confidentiality of [its members'] medical and financial information."[25] The policy also claims that Premera would "protect [members'] personal information in a variety of ways."[26] "For example, we authorize access to your personal information by our employees and business associates only to the extent necessary to conduct our business of serving you, such as

[25] Premera, *supra* note 1.
[26] *Id.*

PHILLIPS LAW FIRM PLLC
17410 133rd Ave NE, Suite 301, Woodinville WA 98072
Tel: (425) 482-1111 Fax: (425) 482-6653

paying your claims. We take steps to secure our buildings and electronic systems from unauthorized access. We train our employees on our written confidentiality policy and procedures and employees are subject to discipline if they violate them. Our privacy policy and practices apply equally to personal information about current and former members; we will protect the privacy of your information even if you no longer maintain coverage through us."[27]

62. Premera's privacy policies constitute an agreement between (1) Premera and (2) its health plan members and employees.

63. Premera has breached its agreement with class members to protect their personal information by (1) failing to implement security measures designed to prevent this attack even though the healthcare industry has been repeatedly warned about the risk of cyber-attacks, and (2) failing to employ security protocols to detect the unauthorized network activity.

64. Plaintiff and class members have been damaged by Premera's breach of its obligations because their personal information has been compromised and they are at and increased risk for future identity theft and fraudulent activity on their financial accounts. Class members have also lost money and property by purchasing credit monitoring services they would not otherwise had to but for Premera's unlawful and unfair conduct.

65. Plaintiff, individually and on behalf of the members of the Nationwide Class, seeks (a) damages suffered by members of the class, (b) equitable relief, and (c) injunctive relief requiring Premera to implement safeguards consistent with its contractual promises.

66. Plaintiff, individually and on behalf of the members of the class, also seeks reasonable attorneys' fees and costs under applicable law including Federal Rule of Civil Procedure 23.

FOURTH CAUSE OF ACTION

Negligence

67. Plaintiff incorporates the above allegations by reference.

68. Plaintiff brings this cause of action on behalf of the Nationwide Class whose personal information was compromised as a result of the data breach publicized in March 2015.

[27] *Id.*

PHILLIPS LAW FIRM PLLC
17410 133rd Ave NE, Suite 301, Woodinville WA 98072
Tel: (425) 482-1111 Fax: (425) 482-6653

69. In collecting the personal information of its current and former health insurance plan members and employees, Premera owed Plaintiff and members of the class a duty to exercise reasonable care in safeguarding and protecting that information. This duty included, among other things, maintaining and testing Premera's security systems and taking other reasonable security measures to protect and adequately secure the personal data of Plaintiff and the class from unauthorized access and use. Premera's security system and procedures for handling the personal information of its current and former health insurance plan members and employees were intended to affect Plaintiff and the class. Premera was aware that by taking such sensitive information of its health insurance plan members and employees, it had a responsibility to take reasonable security measures to protect the data from being stolen and, in the event of theft, easily accessed.

70. The duty Premera owed to Plaintiff and members of the class to protect their personal information is also underscored by the Revised Code of Washington and HIPAA, which recognize the importance of maintaining the confidentiality of personal information and were established to protect individuals from improper disclosure of their personal information.

71. Additionally, Premera had a duty to timely disclose to Plaintiff and members of the class that their personal information had been or was reasonably believed to have been compromised. Timely disclosure is appropriate so that Plaintiff and members of the class could, among other things, report the theft of their Social Security numbers to the Internal Revenue Service, monitor their credit reports for identity fraud, and undertake appropriate measures to mitigate the risk of fraudulent cash withdrawals or unauthorized transactions on their bank accounts.

72. There is a very close connection between Premera's failure to take reasonable security standards to protect its current and former health insurance plan members' and employees' data and the injury to Plaintiff and the class. When individuals have their personal information stolen, they are at risk for identity theft, and need to buy credit monitoring services and purchase credit reports to protect themselves from identity theft.

PHILLIPS LAW FIRM PLLC
17410 133rd Ave NE, Suite 301, Woodinville WA 98072
Tel: (425) 482-1111 Fax: (425) 482-6653

73. Premera is morally to blame for not protecting the data of its current and former health insurance plan members and employees by failing to take reasonable security measures. If Premera had taken reasonable security measures, data thieves would not have been able to take the personal information of millions of current and former Premera health insurance plan members and Premera employees.

74. The policy of preventing future harm weighs in favor of finding a special relationship between Premera and the class. Premera's health insurance plan members and employees count on Premera as their healthcare provider and/or employer to keep their data safe and in fact are required to share sensitive personal data with Premera as a condition of health plan enrollment and/or employment. If companies are not held accountable for failing to take reasonable security measures to protect their health plan members' and employees' personal information, they will not take the steps that are necessary to protect against future data breaches.

75. It was foreseeable that if Premera did not take reasonable security measures, the data of Plaintiff and members of the class would be stolen. Major corporations, particularly those in the healthcare industry, like Premera, face a higher threat of security breaches than other companies due in part to the large amounts and type of data they possess. Premera should have known to take precautions to secure its health plan members' and employees' data, especially in light of recent data breaches and warnings regarding cyber-attacks and network vulnerability in the healthcare industry.

76. Premera breached its duty to exercise reasonable care in protecting the personal information of Plaintiff and the class by failing to implement and maintain adequate security measures to safeguard its health plan members' and employees' personal information, failing to monitor its systems to identify suspicious activity, and allowing unauthorized access to the personal information of Plaintiff and the class.

77. Premera breached its duty to timely notify Plaintiff and the class about the data breach. Premera has failed to issue any timely notice to its current and former health plan members and employees affected by the breach. Additionally, Premera was, or should have been, aware of breaches in its network security as early as May 5, 2014.

PHILLIPS LAW FIRM PLLC
17410 133rd Ave NE, Suite 301, Woodinville WA 98072
Tel: (425) 482-1111 Fax: (425) 482-6653

78. But for Premera's failure to implement and maintain adequate security measures to protect its current and former health plan members' and employees' personal information and failure to monitor its systems to identify suspicious activity, the personal information of Plaintiff and members of the class would not have been stolen, and they would not be at a heightened risk of identity theft in the future.

79. Premera's negligence was a substantial factor in causing harm to Plaintiff and members of the class.

80. As a direct and proximate result of Premera's failure to exercise reasonable care and use commercially reasonable security measures, the personal information of current and former Premera health plan members and Premera employees was accessed by unauthorized individuals who could use the information to commit identity fraud, medical fraud, or financial fraud. Plaintiff and the class face a heightened risk of identity theft in the future.

81. Members of the class have also suffered economic damages, including the purchase of credit monitoring services they would not have otherwise purchased.

82. Neither Plaintiff nor other members of the class contributed to the security breach, nor did they contribute to Premera's employment of insufficient security measures to safeguard health plan members' and employees' personal information.

83. Plaintiff and the class seek compensatory damages and punitive damages with interest, the costs of suit and attorneys' fees, and other and further relief as this Court deems just and proper.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the proposed classes, requests that the Court:

a. Certify this case as a class action on behalf of the classes defined above, appoint Marianna Powers as class representative, and appoint Girard Gibbs and Phillips Law as class counsel;

PHILLIPS LAW FIRM PLLC
17410 133rd Ave NE, Suite 301, Woodinville WA 98072
Tel: (425) 482-1111 Fax: (425) 482-6653

b. Award declaratory, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and other class members;

c. Award damages, including actual and statutory, damages and restitution to Plaintiff and class members in an amount to be determined at trial;

d. Award Plaintiff and class members their reasonable litigation expenses and attorneys' fees;

e. Award Plaintiff and class members pre- and post-judgment interest, to the extent allowable; and

f. Award such other and further relief as equity and justice may require.

Dated: April 9, 2015

Respectfully Submitted,

PHILLIPS LAW FIRM PLLC

By: /s/ R. Glenn Phillips

R. Glenn Phillips (SBN 14220)
17410 133rd Ave NE, Suite 301
Woodinville WA 98072
Telephone: (425) 482-1111
Facsimile: (425) 482-6653
glenn@justiceforyou.com

Daniel C. Girard, *pro hac vice forthcoming*
Eric H. Gibbs, *pro hac vice forthcoming*
GIRARD GIBBS LLP
601 California Street, 14th Floor
San Francisco, California 94108
Telephone: (415) 981-4800
Facsimile: (415) 981-4846
dcg@girardgibbs.com
ehg@girardgibbs.com

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury for all issues so triable.

Dated: April 9, 2015

Respectfully Submitted,

PHILLIPS LAW FIRM PLLC

By: /s/ R. Glenn Phillips

R. Glenn Phillips (SBN 14220)
17410 133rd Ave NE, Suite 301
Woodinville WA 98072
Telephone: (425) 482-1111
Facsimile: (425) 482-6653
glenn@justiceforyou.com

Daniel C. Girard, *pro hac vice forthcoming*
Eric H. Gibbs, *pro hac vice forthcoming*
GIRARD GIBBS LLP
601 California Street, 14th Floor
San Francisco, California 94108
Telephone: (415) 981-4800
Facsimile: (415) 981-4846
dcg@girardgibbs.com
ehg@girardgibbs.com